Les établissements scolaires également victimes de ransomwares

Les établissements scolaires également victimes de ransomwares

Après les hôpitaux, les ransomwares s'attaquent de plus en plus aux établissements scolaires. Retour sur plusieurs cas aux Etats-Unis.

Les ransomwares sont devenus la plaie des responsables sécurité des entreprises ou des administrations. On peut se remémorer le témoignage du RSSI de l'AFP qui en a fait l'expérience. Le secteur hospitalier a été particulièrement touché avec différents exemples. Le plus symptomatique est le Hollywood Presbyterian Medical Center de Los Angeles qui a été obligé de payer 17 000 dollars en bitcoin pour retrouver l'usage de son réseau.

Certains payent la rançon

Après les hôpitaux, les ransomwares s'intéressent à une autre cible : les écoles. Plusieurs cas ont été recensés aux Etats-Unis. En février dernier, plusieurs écoles primaires du Horry County en Caroline du Sud ont été victimes d'un rançongiciel qui a bloqué 25 serveurs. Immédiatement après avoir été alertée par les enseignants, l'équipe IT a débranché les serveurs affectant ainsi les services en lignes des écoles. Après enquête, la porte d'entrée du malware était un vieux serveur non mis à jour. Toujours est-il que les responsables de l'école ont se sont vus réclamer 0,8 bitcoin par ordinateur soit un total de 20 bitcoins (environ 7600 euros). Malgré l'aide du FBI, le conseil d'administration du campus a décidé de payer la rançon demandée.

D'autres non

D'autres ont décidé de ne pas payer la rançon comme dans le cadre du Oxford School District dans le Mississipi. En février dernier aussi, ce réseau de 8 campus a été infecté par un rançongiciel réclamant environ 9000 dollars pour un retour à la normal. Le superintendant de l'établissement, Brian Harvey, a préféré ne pas payer et s'est concentré sur la récupération des données. Dans un entretien accordé à HottyDotty, il précise que « nous avons restauré à partir d'une sauvegarde ». Mais les dégâts étaient importants. « Je ne sais pas combien de données nous avons perdu. Je peux dire que nous avons perdu la plupart des serveurs Windows. La chose la plus importante a été de tout effacer et de tout réinstaller depuis la sauvegarde. » L'attaque a privé les établissements d'Internet pendant plus d'une journée. Les 4 premiers jours après l'attaque ont été focalisés sur la récupération du système des carnets de notes des élèves. D'autres applications ont souffert comme les reporting ou le recrutement des agents. Au final, deux semaines ont été nécessaires pour tout remettre à peu près d'aplomb : les sites web, la gestion de la cafeteria, ainsi que des plateformes pour l'éduction comme PowerSchool et Schoology.

Les parents d'élève s'inquiètent

Autre affaire, le Texas School District qui gère une vingtaine d'établissements. Un ransomware a infecté le réseau, provoquant le blocage de plusieurs fichiers. La direction du district s'est voulue rassurante en expliquant que seule une petite partie des informations est concernée par le blocage. Ce dernier porte néanmoins sur un volume de 2,5 To de données. Les responsables ont choisi de ne pas payer la rançon demandée par les cybercriminels. « Nous avons réussi à effacer les fichiers chiffrés et à réinstaller données à partir d'une sauvegarde », précise un porte-parole du district. Un cas similaire à celui du Mississipi qui inquiète les parents d'élèves. « Ils [NDLR les établissements] détiennent des actes de naissance, des numéros de sécurité sociale ou des données médicales comme les vaccins », souligne une des parents d'élèves.

En France, aucun cas n'a été relevé ou publié sur des expositions à des ransomwares. Les écoles, universités et autres établissements scolaires font partie de cibles privilégiés par les cybercriminels. Obsolescence des parcs informatiques, système IT peu mis à jour, les pirates se ont trouvé un terrain de jeu grandeur nature pour tester et peaufiner leurs attaques. Les sommes demandées restent modestes, un signe selon les spécialistes pour reconnaître le degré de résistance des victimes à payer la rançon. En tout cas, les exemples américains doivent alerter les établissements bancaires européens et français sur les risques des ransomwares… [Lire la suite]

Réagissez à cet article

Source : *Les ransomwares prennent le chemin des écoliers*